REMARKS

Claims 1, 3-5, 7-8, 10, 12-13, and 15 are amended, no claims are canceled, and no claims are added; as a result, claims 1-15 are now pending in this application.

No new matter has been added through the amendments to claims 1, 3-5, 7-8, 10, 12-13, and 15.

With respect to claim 1, claim 1 specifies that the content player comprises a decryption device, based on claim 3 as originally filed. Claim 1 has also been amended to specify a secure device arranged to transform the secure device data into information required to decrypt the encrypted data. Basis for this amendment is to be found on page 6, line 12 of the application. The claim now refers to a protected contents structure, based on page 5, line 1. The attribute data are defined as being suitable for finding relevant parts inside the contents structure, based on page 4, last line, of the application as filed. The information retrieved from the secure device data is the information required to decrypt the encrypted data. This was already clear from page 6, line 12 of the application as filed. It follows that the amendments do not extend the subject-matter of claim 1 unduly, whilst resolving the issues raised in respect of claim 1 in paragraph 3.1 of the Office Action.

Claim 3 has been amended in a manner corresponding substantially to claim 1. The passages identified above with regard to claim 1 also provide basis for the amendments to claim 3.

Claim 4 has been amended to clarify the antecedent basis for "said protocol information".

Claim 5 has been amended to refer to claim 4 instead of claim 3. Thus, antecedent basis for the feature "the virtual machine" is now present.

Claim 7 has been amended to remove any perceived lack of clarity. Basis for this amendment is to be found on page 6, lines 26-30 of the application as filed.

Claim 8 has been amended to remove the objection contained in paragraph 3.2 of the Office Action.

Claim 10 has been amended in substantially similar manner to claim 3. The passages identified above also provide basis for the amendments to claim 10

Claims 12 and 13 have been amended to remove the objection in paragraph 3.2 of the Office Action.

Claim 15 has been amended to specify that the secure device is arranged to transform the secure device data into the information required to decrypt the encrypted data, based on page 6, lines 12-13 of the application as filed. Additional amendments serve merely to clarify the claim, including a re-ordering of features.

Claim Objections

Claims 1 and 10 were objected to because of the following informalities: claim 1 recites: a control device for providing "a protected contents", which needs to be revised. Claim 10 also recites, receiving "a protected contents."

Claim 1 has been amended to include, "providing a protected contents structure." Further, claim 10 has been amended to include, "receiving a protected contents structure." Applicant respectfully submits that the objections to claims 1 and 10 have been overcome, and withdrawal of these claim objections is respectfully requested.

§112 Rejection of the Claims

Claims 1-15 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically, the Office Action on page 3 states,

> Regarding claims 1, 3, 10, and 15, the limitation "for retrieving the information to decrypt the encrypted data". There is insufficient antecedent basis for this limitation in the claim. It is not clear whether the retrieving is directed to protocol information or attribute data information or other information recited in the claims. Claims 1, 3, and 10 also recite "the different parts inside the protected contents". There in insufficient antecedent basis for this limitation in the claim. Also, there is insufficient antecedent basis for the limitation "the appropriate protocol". (Emphasis original)

Applicant has amended claim 1, 3, 10, and 15 to overcome each of these rejections. Further, the Office Action on page 4 states,

> Claims 2 and 4 recite "said information protocol", claim 5 recites "the virtual machine", claim 7 recites "said interfaces", claims 8, 12, 13 recite "the type of secure device". There is insufficient antecedent basis for these limitations in the claims.

With respect to these rejections, Applicant submits the following:

The objection to claim 2 on grounds of indefiniteness appears to have been made in error. Claim 2 as currently on file does not recite "said information protocol". It recites "said information on a protocol for communication", for which claim 1 provides antecedent basis.

Claim 4 has been amended to clarify the antecedent basis for "said protocol information".

Claim 5 has been amended to refer to claim 4 instead of claim 3. Thus, antecedent basis for the feature "the virtual machine" is now present.

Claim 7 has been amended to remove any perceived lack of clarity. Basis for this amendment is to be found on page 6, lines 26-30 of the application as filed.

Claim 8 has been amended to remove the objection contained in paragraph 3.2 of the Office Action.

Claims 12 and 13 have been amended to remove the objection in paragraph 3.2 of the Office Action.

For at least the reasons stated above, Applicant respectfully submits that the 35 U.S.C. § 112, second paragraph rejection of claims 1-15 have been overcome. Therefore, withdrawal of the rejection and reconsideration and allowance of claims 1-15 is respectfully requested.

§102 Rejection of the Claims

Claims 3 and 10 were rejected under 35 U.S.C. § 102(e) for anticipation by Glover (U.S. 6,052,780). For at least the reasons stated below, the 35 U.S.C. § 102(e) rejection of claims 3 and 10 cannot stand.

Claim 3

The subject-matter of claim 3 is novel compared to Glover (herein after "D1"), because D1 does not disclose an input for receiving protected contents containing information on a

protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data or a control device programmed to find such information to establish a communication interface between a decryption device and such a secure device.

Instead, D1 discloses a program which communicates with an operating system, called a virtual device driver 52 (column 9, lines 20-21). The program need not be a device driver (column 9, lines 12-13). The virtual device driver, when executed, decrypts that desired digital information (column 9, lines 27-28). Thus, the virtual device driver corresponds in function to a secure device *and* a decryption device. If one regards the known computer system 20 as a content player, then the virtual device driver enables communication *within* the secure device/decryption device, but it does not establish a communication interface *between* a decryption device and a secure device arranged to provide the decryption device with information required for decryption. Indeed, it is stated that unencrypted digital information at no time exists on disk in accessible and complete decrypted form (column 20, lines 58-59). As mentioned above, the known secure disk is a computer readable medium (column 9, lines 10-13), and therefore not arranged to transform the secure device data into information required to decrypt the encrypted data in the content player. In fact, it is not even able to participate in communication across a communication interface, being a purely passive data storage medium.

Claim 10

Claim 10 defines a method such as might be performed by a system according to claim 3. The arguments given above with respect to novelty apply equally to claim 10.

In view of the above, it is submitted that D1 fails to disclosure all of the elements of claims 1 and 10, and accordingly, claims 1 and 10 are allowable. Applicant therefore respectfully requests withdrawal of the 35 U.S.C. 102(e) rejection of claims 3 and 10, and reconsideration and allowance of these claims.

§103 Rejection of the Claims

§ 103 Rejection of claims 1, 2, and 15 (Glover)

Claims 1, 2 and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Glover. For at least the reasons stated below, the 35 U.S.C. § 103(a) rejection of claims 1, 2 and 15 cannot stand.

Claim 1

The system defined in claim 1 differs from that known from Glover (US 6,052,780, hereinafter "D1"), in that D1 does not disclose a protection device for providing information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, a control device for providing a protected contents structure containing said protocol information, or information on an appropriate protocol for establishing a communication interface between the content player and the secure device for retrieving the information required to decrypt the encrypted data.

Instead, D1 discloses a program which communicates with an operating system, called a virtual device driver 52 (column 9, lines 20-21). The program need not be a device driver (column 9, lines 12-13). The virtual device driver, when executed, decrypts that desired digital information (column 9, lines 27-28). Thus, the virtual device driver corresponds in function to a secure device *and* a decryption device. If one regards the known computer system 20 as a content player, then the virtual device driver enables communication *within* the content player, but not *between* a content player and a secure device for retrieving the information required to decrypt the encrypted data in the content player. Indeed, it is stated that unencrypted digital information at no time exists on disk in accessible and complete decrypted form (column 20, lines 58-59). It appears from the Office Action (the rejection of claim 3, in particular) that the secure disk of D1 is to be regarded as a secure device in the sense of claim 1. However, the known secure disk is a computer readable medium (column 9, lines 10-13), and therefore not

arranged to transform the secure device data into information required to decrypt the encrypted data in the content player.

The effect of this difference is that the system according to claim 1 is suitable for implementations wherein the secure device and a decryption device in the content player are separate entities, whereas in the known system, possession of the computer program product is sufficient to access the digital information to be used in a content player. For this reason, the known system requires an additional password to be input by a user (column 21, lines 26-30). Moreover, the known system requires that all functions be executed by a processor on a computer system, whereas the functions of decrypting encrypted data and transforming secure device data into information required to decrypt the encrypted data can be carried out in separate, if necessary dedicated, hardware devices using the invention. Thus, starting from D1, the problem solved by the present invention is to provide a system for providing encrypted data that allows a separation between the functions of decrypting the encrypted data and providing information required to decrypt the encrypted data, whilst retaining versatility in terms of the combinations of devices that perform these functions.

This problem is addresed by the system according to claim 1. Because information on a protocol for communication between a secure device and a content player comprising a decryption device is provided by a protection device, the protected contents structure contains the information needed by the content player comprising the decryption device to communicate with a particular secure device. Thus, versatility in terms of combinations of secure devices and content player is obtained, since the content player is not limited to communicating with secure devices for which it has a pre-configured communication interface. Because the content player is provided with information on a protocol for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data, the content player functions without being able itself to obtain the information required to decrypt the encrypted data from the secure device data in the protected contents structure. In this way, the presence of a secure device is made indispensable. The secure

device thus functions as a token for authorising decryption. Unlike a password, such a token cannot be shared.

The invention is not obviously derivable from D1, because D1 teaches a decryption program that decrypts the encrypted information to provide the desired digital information, upon successful completion of an authorization procedure by the user (column 3, lines 47-51). A platform provider merely provides a computer system with an operating system that has adequate security to define a protected memory area for a process and adequate functionality to execute a decryption program (column 3, lines 63-67). D1 teaches away from using a secure device to enable decryption of the contents towards using a single protected contents structures so that decrypted information does not pass through any device driver, memory resident program or other known logical entity in a computer system (column 4, lines 2-5).

The skilled person is not provided with any suggestion, motivation or incentive to combine D1 with US 6,157,721 (hereinafter: D2). D1 teaches a mechanism which allows a content provider to encrypt digital information without requiring either a hardware or platform manufacturer or a content consumer to provide support for the specific form of decryption (see abstract of D1). Any need for ... a centralised facility ... is eliminated (column 21, lines 7-9). A hardware manufacturer only provides the mechanism to protect the digital information through the operating system (column 21, lines 55-57). In stark contrast thereto, D2 discloses techniques for certifying load modules, wherein protected execution spaces such as protected processing environments can be programmed or otherwise conditioned to accept only those load modules or other executable bearing a digital signature/certificate of an accredited (or particular) verifying authority (column 5, lines 1-5 of D2). Thus, D2 teaches to use a centralised facility, where the provider of the protected processing environment must ensure that the keys for verifying the signature/certificate issued by the verifying authority are present. It follows that the teachings of D1 and D2 are contradictory, and that the skilled person would not combine them.

Moreover, the problem addressed in D2 is to protect a computer-processing environment against potentially harmful computer executables, which is a different problem from the one

objectively derivable on the basis of a comparison between claim 1 and D1. For this reason also, the skilled person would not turn to D2.

Even if the skilled person were to consult D2, he would not find any disclosure of a protection device for providing information on a protocol for communication between the content player and a secure device arranged to transform secure device data into information required to decrypt encrypted data, a control device for providing a protected contents structure containing said protocol information, or information on an appropriate protocol for establishing a communication interface between the content player and the secure device for retrieving the information required to decrypt the encrypted data.

Instead, the load modules disclosed in D2 are shared in their entirety (column 18, lines 3-7), but otherwise compartmentalised (column 18, line 12) to isolate appliances with significantly different work factors (column 18, lines 15-16). There is, in fact, no disclosure of any secure device arranged to transform secure device data into information required to decrypt encrypted data. D2 only describes providing to a protected processing environment the key and one-way hash algorithm for verifying a signature by means of a secure key exchange protocol (column 13, lines 60-67). Thus, D2 only teaches an alternative to retrieving information required to decrypt encrypted data by establishing a communication interface to a secure device using protocol information received with the encrypted data in a protected contents structure.

Claim 2

Claim 2 depends from claim 1, and so includes all of the elements recited in claim 1. For at least the reasons stated above with regards to claim 1, D1 fails to disclose all of the elements included in claim 2. Therefore, the 35 U.S.C. 103(a) rejection of claim 2 cannot stand.

Claim 15

The method of claim 15 differs from that known from D1 in that D1 does not disclose a method for broadcasting protected contents, a method comprising providing information on a protocol for communication between a content player and a secure device arranged to transform

secure device data into information required to decrypt the encrypted data, providing protected contents containing the protocol information, or broadcasting the protected contents. Instead of a method of broadcasting protected contents, D1 describes (column 22, lines 2-10) a process that could be used for on-line or live use of digital information. A movie could be retrieved on demand and recorded by a consumer. A set-top box could receive the digital information, decrypt it, and then re-encrypt and store the information using, for example, a hardware identifier of the set-top box. It is noted that video-on-demand is not the same as broadcasting protected contents. Video-on-demand is implemented using a one-to-one communication channel, whereas broadcasting is characterised by one-to-many communication. Instead of providing information on a protocol for communication between a content player and a secure device arranged to transform secure device data into information required to decrypt the encrypted data, providing protected contents containing the protocol information and broadcasting the protected contents, D1 discloses a program which communicates with an operating system, called a virtual device driver 52 (column 9, lines 20-21). The program need not be a device driver (column 9, lines 12-13). The virtual device driver, when executed, decrypts that desired digital information (column 9, lines 27-28). Thus, the virtual device driver corresponds in function to a secure device *and* a content player. If one regards the known computer system 20 as a content player, then the virtual device driver enables communication *within* the content player, but not *between* a content player and a secure device for retrieving the information required to decrypt the encrypted data in the content player.

The effect of this difference is that the known process requires individualisation of content as it is received, in order to prevent users from passing it on. By contrast, the method according to claim 15 allows for a separation of the functions of decryption of encrypted data and generation of the information required to decrypt the encrypted data, using a secure device as an access token. The presence of a secure device is required to decrypt the data encrypted using the encryption algorithm, although the content player need not be pre-configured for communication with the secure device being used.

The skilled person has no reason to combine the disclosure of D1 with that of D2 for the reasons outlined above with regard to claim 1. Moreover, D2 does not disclose the features of claim 15 identified above as absent from D1. D2 does not unambiguously disclose broadcasting protected contents. Instead, it refers only to the "distribution of load modules" (column 20, line 65 and further), which involves determining whom the load module should be distributed to (column 20, lines 66-67). This suggests that the load modules are addressed to individual devices, as does the fact that differently signed load modules are distributed to different device classes (claim 1 of D2). Instead of providing information on a protocol for communication between the content player and a secure device arranged to transform secure device data into information required to decrypt encrypted data, providing protected contents containing the protocol information, and attribute data comprising information to find in the protected contents information on an appropriate protocol for establishing a communication interface between the content player and the secure device for retrieving the information required to decrypt the encrypted data, D2 discloses load modules, shared in their entirety (column 18, lines 3-7), but otherwise compartmentalised (column 18, line 12) to isolate appliances with significantly different work factors (column 18, lines 15-16). There is, in fact, no disclosure of any secure device arranged to transform secure device data into information required to decrypt encrypted data. D2 only describes providing to a protected processing environment the key and one-way hash algorithm for verifying a signature by means of a secure key exchange protocol (column 13, lines 60-67). Thus, D2 only teaches an alternative to providing protected contents containing information on a protocol for communication between a content player and a secure device arranged to transform the secure device data into the information required to decrypt the encrypted data.

For these reasons, the subject-matter of claim 15 is not obvious having regard to D1 and D2, either.

Applicant respectfully requests withdrawal of the § 103(a) rejection of claims 1-2 and 15, and reconsideration and allowance of these claims.

§ 103 Rejection of claims 4-9 and 11-14 (Glover/Shear et al)

Claims 4-9 and 11-14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over US Patent 6,052,780 Glover to Glover (again, hereinafter "D1") in view of US Patent 6,157,721 to Shear et al (hereinafter "D2"). For at least the reasons stated below, the 35 U.S.C. § 103(a) rejection of claims 4-9 and 11-14 cannot stand.

Claims 4-9

Claims 4-9 depend from claim 3, and so include all of the elements recited in claim 3. Applicant submits that for at least the reasons stated above with respect to claim 3, claims 4-9 are not obvious in view of D1 and D2. Further, arguments relating to obviousness have been set out above with regard to claim 1 and apply equally to the system defined in claim 3.

Because the proposed combination of D1 and D2 fails to teach all of the elements of claims 4-9 and because the skilled person has anyway no reason or motivation to combine their teachings, it is submitted that the invention defined in claims 4-9 is not obvious. In view of the remarks above, Applicant respectfully requests withdrawal of the rejections and reconsideration and allowance of claims 4-9.

Claims 11-14

Claims 11-14 depend from claim 10, and so include all of the elements recited in claim 10. Applicant submits that for at least the reasons stated above with respect to claim 10, claims 11-14 are not obvious in view of D1 and D2. Further, arguments relating to obviousness have been set out above with regard to claim 3 and apply equally to the system defined in claim 10.

Because the proposed combination of D1 and D2 fails to teach all of the elements of claims of claims 11-14 and because the skilled person has anyway no reason or motivation to combine their teachings, it is submitted that the invention defined in claims 11-14 is not obvious. In view of the remarks above Applicant respectfully requests withdrawal of the rejections and reconsideration and allowance of claims 11-14.

CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at 408-278-4042 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

WILHELMUS GERARDUS PETRUS MOOIJ

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-278-4042

Date 01/20/06

By _____
André L. Marais
Reg. No. 48,095

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 20 day of January, 2006.

Dawn R. Shaw _____ Dawn R. Shaw

Name Signature